KARL STORZ SE & Co. KG • Postfach 230 • 78503 Tuttlingen/Germany

January 14th, 2022

Security Notice CVE-2021-44228 and CVE-2021-4104
Apache Log4j Logging Tool Remote Execution Vulnerability

Dear Sir or Madam,

KARL STORZ is aware of and currently monitoring the Apache Log4j (commonly referred to as "Log4Shell") Logging Tool Remote Execution Vulnerability (CVE-2021-44228) and its related Java Appender vulnerability (CVE-2021-4104). These vulnerabilities were discovered on or about December 9th, 2021. To date, there have been no reported exploitations of these vulnerabilities in KARL STORZ products.

Regarding CVE-2021-44228:
We can assure you that all of our **currently supported** KARL STORZ medical products and their accompanying infrastructures do not utilize Apache Log4j **2.x** and are **unaffected** by the vulnerability **CVE-2021-44228**.

Regarding CVE-2021-4104:
Although KARL STORZ has had no reports of this vulnerability being exploited on a KARL STORZ product, older non-supported versions of our StreamConnect® product with software versions 4.1.3 or lower and SCENARA® with software version 3.0 use the Apache Log4j 1.x and **may be affected** by CVE-2021-4104. In the products default configuration, the vulnerability cannot be exploited. The Apache Log4j 1.x used by these products is **unaffected** by the CVE-2021-44228.

A list of KARL STORZ affected products and a statement of which vulnerabilities are applicable can be found in Appendix I.

KARL STORZ recommends the following steps:

Mitigation

- Remove older version of the StreamConnect and/or SCENARA.media system from the network.

Solution

- Upgrade the StreamConnect and/or SCENARA.media system to the most current software version

Employ Good Network Hygiene Practices

- Ensure data has been backed up and stored according to your individual processes and disasterrecovery procedures.
- Execute updates to malware protection, where available.

Customers that maintain Virtual Machine (VM) system patches independent of KARL STORZ patch release should ensure these actions are performed to maintain the correct security posture of the system(s).

For more information on this CVE, please follow the link below:
https://nvd.nist.gov/vuln/detail/CVE-2021-44228
https://nvd.nist.gov/vuln/detail/CVE-2021-4104

If you have questions, please contact your KARL STORZ sales representative, or contact us at the following address: security-docs@karlstorz.com

Revision History

Version	Date	Comment
1.0	2021-12-17	Initial advisory
1.1	2021-12-20	Added information on CVE-2021-4104
1.2	2022-01-14	Updated list of affected articles.

Annex I - List of affected products

Article/Model	Product Description	Software Version	CVE-2021-44228 “Log4Shell”	CVE-2021-4104
WUIS3529	StreamConnect®	Version v4.1.3 or lower	**Not Affected**	**Affected**
WUIS3529	StreamConnect®	Version 4.1.4 or higher	**Not Affected**	**Not Affected**
WS11140	SCENARA®. media	Version 3.0	**Not Affected**	**Affected**
WS11140	SCENARA®. media	Version 3.1 or higher	**Not Affected**	**Not Affected**
WS111	SCENARA.core	All versions	**Not Affected**	**Affected**

All other KARL STORZ products are unaffected by CVE-2021-44228 and CVE-2021-4104.